

TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371

01245/TL

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/830378

INTERNATIONAL APPLICATION NO.  
PCT/FR99/02639INTERNATIONAL FILING DATE  
28 October 1999PRIORITY DATE CLAIMED  
29 October 1998

TITLE OF INVENTION DEVICE AND METHOD FOR MAKING AN INTEGRATED CIRCUIT SECURE

APPLICANT(S) FOR DO/EO/US Eric GERBAULT

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☒ has been transmitted by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☐ have been transmitted by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.  
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:

Form PCT/IB/308

CHANGE OF CORRESPONDENCE ADDRESS  
APPLICATION  
ASSIGNMENT INFORMATION FOR  
PUBLICATION

Express Mail Mailing Label No.:

EL 759 972 166 US

Date of Deposit

April 25, 2001

I hereby certify that this paper and any papers identified herein  
is being deposited with the United States Postal Service "Express  
Mail Post Office to Addressee" service under 37 CFR 1.10 on the  
date indicated above and is addressed to the Assistant  
Commissioner for Patents, Washington, D.C. 20231

*Yolanda Usher*  
Yolanda Usher

U.S. APPLICATION NO. (USPTO) <b>09/830378</b>		INTERNATIONAL APPLICATION NO. <b>PCT/FR99/02639</b>		ATTORNEY'S DOCKET NUMBER <b>01245/TL</b>	
17. <input checked="" type="checkbox"/> The following fees are submitted: <b>BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)):</b> Search Report has been prepared by the EPO or IPO ..... \$860.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) ..... \$690.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) ..... \$750.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... \$1,000.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) ..... \$100.00  <b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>				<b>CALCULATIONS</b> PTO USE ONLY	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	8 - 20 =	0	x 18.00	\$ 0	
Independent claims	2 - 3 =	0	x 80.00	\$ 0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			x 270.00	\$	
<b>TOTAL OF ABOVE CALCULATIONS =</b>				\$ 860.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).				\$	
<b>SUBTOTAL =</b>				\$ 860.00	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	
<b>TOTAL NATIONAL FEE =</b>				\$ 860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property				\$	
<b>TOTAL FEES ENCLOSED =</b>				\$ 860.00	
				Amount to be:	\$
				refunded	\$
				charged	\$

- a. ☒ A check in the amount of \$ 860.00 to cover the above fees is enclosed.
- b. ☐ Please charge my Deposit Account No. \_\_\_\_\_ in the amount of \$ \_\_\_\_\_ to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1378. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

FRISHAUF, HOLTZ, GOODMAN, LANGER & CHICK, P.C.  
767 Third Avenue - 25th Floor  
New York, NY 10017-2023

Tel. No. (212) 319-4900  
Fax No. (212) 319-5101

Date: April 25, 2001

*Thomas Langer*  
SIGNATURE:

Thomas Langer

NAME

27,264

REGISTRATION NUMBER

09/830378


JC03 Rec'd PCT/PTO 25 APR 2001

Attorney Docket No. 01245/TL

Express Mail Mailing Label  
No.: EL 759 977 166 US  
Date of Deposit: April 25, 2001

**IN THE UNITED STATES PATENT  
AND TRADEMARK OFFICE**

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Asst. Commissioner for Patents, Washington, D.C. 20231

  
Yolanda Usher

Applicant(s): Eric GERBAULT

Serial No. : Not Yet Assigned (U.S. Natl.  
Phase of PCT/FR99/02639 filed  
10/28/99)

Filed : CONCOMITANTLY HEREWITH

For : DEVICE AND METHOD FOR MAKING  
AN INTEGRATED CIRCUIT SECURE

Art Unit :  
Examiner :

**PRELIMINARY AMENDMENT**

**BOX PCT**

Asst. Commissioner for Patents  
Washington, D.C. 20231

S I R :

Please amend the above-identified application as follows:

**IN THE SPECIFICATION**

Please insert the following as the first sentence of the above-identified application:

--This application is a U.S. National Phase Application under 35 USC 371 of International Application PCT/FR99/02639 (not published in English) filed 28 October 1999.--

2005030600

Page 1, before the paragraph starting on line 2, insert the following heading:

--FIELD OF THE INVENTION--

Between lines 7 and 8, insert the heading

--BACKGROUND OF THE INVENTION--.

Page 2, between lines 10 and 11, insert the heading

--SUMMARY OF THE INVENTION--.

Page 3, between lines 10 and 11, insert the heading

--BRIEF DESCRIPTION OF THE DRAWINGS--.

Page 3, between lines 27 and 28, insert the heading

--DETAILED DESCRIPTION OF THE DRAWINGS--.

IN THE CLAIMS

Change the heading to --I CLAIM--.

Please amend claims 1-8 as follows (see attachment for details of changes):

1. (Amended) An integrated circuit device containing a memory area that comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks, N being an integer greater than 1, characterized in that

5 said memory area has M replicas, M being an integer greater than  
1, of x program code blocks, x being an integer comprised between  
1 and N, wherein said replicas reside at different addresses  
within said memory area, and in that said device comprises  
selection means for randomly selecting one replica of at least  
10 one of the x blocks as a block replica to be used when executing  
said program.

2. (Amended) A device according to claim 1, characterized  
in that the sums of bit values of at least two addresses among  
the set of addresses of one replicated block and its M replicas  
are different.

3. (Amended) A device according to claim 1, characterized  
in that, among the set of addresses of one replicated block and  
its M replicas, one address resides within the program memory and  
another address resides within the data memory.

4. (Amended) A device according to claim 1, characterized  
in that it comprises controller means for randomly scheduling  
block execution.

5. (Amended) A method for making secure an integrated  
circuit device containing a memory area, which comprises, on the  
one hand, a data memory and a program memory, and on the other  
hand, a program having N code blocks, N being an integer greater

5 than 1, characterized in that said method comprises the steps of:

- generating, within said memory area, M replicas, M being an integer greater than 1, of x program code blocks, x being an integer comprised between 1 and N, wherein said replicas reside at different addresses within said memory area, and

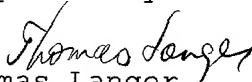
10 - randomly selecting one replica of at least one of the x blocks as a block replica to be used when executing said program.

6. (Amended) A method according to claim 5, characterized in that said method comprises the additional step of selecting the sums of bit values of at least two addresses among the set of addresses of one replicated block and its M replicas in such a way that they are different.

7. (Amended) A method according to claim 5, characterized in that, among the set of addresses of a replicated block and its M replicas, an address is selected within the program memory and another address is selected within the data memory.

8. A method according to claim 5, characterized in that said method comprises the additional step of randomly scheduling block execution.

Respectfully submitted,

  
Thomas Langer  
Reg. No. 27,264

Frishauf, Holtz, Goodman, Langer & Chick, P.C.  
767 Third Avenue - 25th Floor  
New York, New York 10017-2032  
Tel. No. (212) 319-4900  
Facsimile No. (212) 319-5101  
TL:yu

- 1 -

## DEVICE AND METHOD FOR MAKING AN INTEGRATED CIRCUIT SECURE

5      This application is a U.S. National Phase Application  
under 35 USC 371 of International Application  
PCT/FR99/02639 (not published in English) filed 28 October  
1999.

FIELD OF THE INVENTION

10      The present invention relates to an integrated circuit  
device containing a memory area, which comprises, on the  
one hand, a data memory and a program memory, and on the  
other hand, a program having n code blocks  $B_i$  ( $i = 1, \dots,$   
N). It further relates to a method for making such a device  
secure.

BACKGROUND OF THE INVENTION

15      Integrated circuit devices of this kind are most often  
used in applications where confidential information storing  
and processing security is essential. These can for example  
be electronic component-carrying cards for applications  
relating to the fields of health, mobile telephony, or also  
banking applications.

20      Such cards comprise an integrated circuit which  
conventionally includes a controller for (for example a  
central processing unit or CPU) managing and distributing,  
through bus lines, data or address information that is  
stored within the memory area of said cards. This  
25      integrated circuit having bus lines consumes electrical  
power, in particular when these bus lines are used to carry  
logical 1 information.

30      Also, the intensity of the electrical current used by  
an electronic component-carrying card varies with time, in  
particular because of the different values of data or  
addresses transiting over said bus lines in the card. The  
current change as a function of time is an electrical  
signature of the card's activity and therefore, analyzing  
said signature is indicative of said activity. Thereby, by  
35      means of an analysis of the electrical signature, forgers,  
for example, can easily follow a succession of operations

contained in the different code blocks of the program of said card and therefore, can access the confidential information contained in this card.

5 In order to make the analysis of the electrical signature more complex to forgers, the state of the art suggests providing auxiliary devices for generating spurious signals that are added to the electrical signature of said electronic component-carrying card's activity. Although they make the electrical signature analysis more  
10 delicate, such auxiliary devices are slow because they monopolize some of the card's resources, which resources are already used for executing other operations specific to the card and consume more current because they include electronic components that require electrical power for their operation.

#### SUMMARY OF THE INVENTION

Thus, one technical problem to be solved by the present invention is that of providing an integrated circuit device containing a memory area that comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks  $B_i$  ( $i=1, \dots, N$ ), as well as a method for making such a device secure, for obtaining an electrical signature in such a way that said signature is difficult to analyze and which further requires little  
25 power and time consumption, for example due to auxiliary devices appropriating the device's own resources.

According to a first object of the present invention, a solution to the technical problem posed is characterized in that said memory area of said integrated circuit device comprises M replicas  $C_j$  ( $j = 1, \dots, M$ ) having x program code blocks  $B_i$  ( $x = 1, \dots, N$ ), said replicas residing at different addresses within said memory area, and in that said device comprises selection means for randomly selecting a replica  $C_j$  of at least one of the x blocks  $B_i$ ,  
30 as a block replica to be used when executing said program.

35 According to a second object of the present invention, this solution is characterized in that the securing method comprises the steps of:



- creating, within said memory area, M replicas  $C_j$  ( $j = 1, \dots, M$ ) of  $x$  program code blocks  $B_i$  ( $x = 1, \dots, N$ ), wherein said replicas reside at different addresses within said memory area, and

5 - randomly selecting one replica  $C_j$  of at least one of the  $x$  blocks  $B_i$ , as a block replica to be used when executing said program.

10 Therefore, as explained in detail below, the device according to the invention prevents forgery by making the analysis of the electrical signatures very difficult to analyze by such forgery, taking advantage of the fact that said electrical signature varies, in particular, as a function of the values transiting over said device bus lines.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Other features and advantages of the invention will become apparent from the following description of preferred embodiments of the present invention, provided by way of non-limiting examples, in reference to the appended Figures, in which:

Fig. 1 illustrates an integrated circuit device, such as, for example, an electronic component-carrying card.

Fig. 2 illustrates a memory area in the card of Fig. 1.

Fig. 3 illustrates bus lines in the card of Fig. 1.

25 Fig. 4 illustrates the memory area of Fig. 2 restricted to code block  $B_i$ .

Fig. 5 illustrates addressing of a code block and its replicas within the card of Fig. 1.

30 Fig. 6 illustrates a distribution of a code block and its replicas within a memory area of Fig. 2.

Fig. 7 illustrates another distribution of a code block and its replicas within the memory area of Fig. 2.

#### DETAILED DESCRIPTION OF THE INVENTION

35 Fig. 1 shows an integrated circuit device 10, for example an electronic component-carrying card.

Card 10 includes a controller (for example a central processing unit or CPU), a memory area 12 including a data memory 14 and a program memory 15, and a terminal block 13

AMENDED CLAIMS SHOWING CHANGES MADE TO CLAIMS

(U.S. Natl. Phase of Appln  
No. PCT/FR98/02639).

[CLAIMS] I CLAIM

1. (Amended) An integrated circuit device containing a memory area that comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks, N being an integer greater than 1 [Bi (i = 1, ..., N)], characterized in that said memory area has M replicas [Cj (j = 1, ..., M)], M being an integer greater than 1, of x program code blocks [Bi (x = 1, ..., N)], x being an integer comprised between 1 and N, wherein said replicas reside at different addresses within said memory area, and in that said device comprises selection means for randomly selecting one replica [Cj] of at least one of the x blocks [Bi], as a block replica to be used when executing said program.

2. A device according to claim 1, characterized in that the sums of bit values of at least two addresses among the set of addresses of one replicated block [Bi] and its M replicas [Cj] are different.

3. (Amended) A device according to [any preceding claim] claim 1, characterized in that, among the set of addresses of one replicated block [Bi] and its M replicas, one address resides within the program memory and another address resides within the data memory.

4. (Amended) A device according to [any preceding claim] claim 1, characterized in that it comprises controller means for randomly scheduling block execution.

5. (Amended) A method for making secure an integrated circuit device containing a memory area, which comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks, N being an integer greater than 1 [Bi (i = 1, ..., N)], characterized in that said method comprises the steps of:

- generating, within said memory area, M replicas [Cj (j = 1, ..., M)], M being an integer greater than 1, of x program code blocks [Bi (x = 1, ..., N)], x being an integer comprised between 1 and N, wherein said replicas reside at different addresses within said memory area, and

- randomly selecting one replica [Cj] of at least one of the x blocks [Bi], as a block replica to be used when executing said program.

6. (Amended) A method according to claim 5, characterized in that said method comprises the additional step of selecting the sums of bit values of at least two addresses among the set of addresses of one replicated block [Bi] and its M replicas [Cj] in such a way that they are different.

7. (Amended) A method according to [claims 5 or 6] claim 5, characterized in that, among the set of addresses of a replicated block [Bi] and its M replicas, an address is selected within the program memory and another address is selected within the data memory.

8. A method according to [claims 5, 6 or 7] claim 5, characterized in that said method comprises the additional step of randomly scheduling block execution.

H/PRF

09/830378

JC03 Rec'd PCT/PTO 25 APR 2001

- 1 -

DEVICE AND METHOD FOR MAKING AN INTEGRATED CIRCUIT SECURE

5 The present invention relates to an integrated circuit device containing a memory area, which comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having  $n$  code blocks  $B_i$  ( $i = 1, \dots, N$ ). It further relates to a method for making such a device secure.

Integrated circuit devices of this kind are most often used in applications where confidential information storing and processing security is essential. These can for example be electronic component-carrying cards for applications relating to the fields of health, mobile telephony, or also banking applications.

20 Such cards comprise an integrated circuit which conventionally includes a controller for (for example a central processing unit or CPU) managing and distributing, through bus lines, data or address information that is stored within the memory area of said cards. This integrated circuit having bus lines consumes electrical power, in particular when these bus lines are used to carry logical 1 information.

25 Also, the intensity of the electrical current used by an electronic component-carrying card varies with time, in particular because of the different values of data or addresses transiting over said bus lines in the card. The current change as a function of time is an electrical signature of the card's activity and therefore, analyzing said signature is indicative of said activity. Thereby, by means of an analysis of the electrical signature, forgers, 30 for example, can easily follow a succession of operations contained in the different code blocks of the program of said card and therefore, can access the confidential information contained in this card.

35 In order to make the analysis of the electrical signature more complex to forgers, the state of the art

5 suggests providing auxiliary devices for generating  
spurious signals that are added to the electrical signature  
of said electronic component-carrying card's activity.  
Although they make the electrical signature analysis more  
delicate, such auxiliary devices are slow because they  
monopolize some of the card's resources, which resources  
are already used for executing other operations specific to  
the card and consume more current because they include  
electronic components that require electrical power for  
their operation.

10 Thus, one technical problem to be solved by the present  
invention is that of providing an integrated circuit device  
containing a memory area that comprises, on the one hand,  
a data memory and a program memory, and on the other hand,  
a program having N code blocks  $B_i$  ( $i=1, \dots, N$ ), as well  
as a method for making such a device secure, for obtaining  
an electrical signature in such a way that said signature  
is difficult to analyze and which further requires little  
power and time consumption, for example due to auxiliary  
devices appropriating the device's own resources.

20 According to a first object of the present invention,  
a solution to the technical problem posed is characterized  
in that said memory area of said integrated circuit device  
comprises M replicas  $C_j$  ( $j = 1, \dots, M$ ) having x program  
code blocks  $B_i$  ( $x = 1, \dots, N$ ), said replicas residing at  
different addresses within said memory area, and in that  
said device comprises selection means for randomly  
selecting a replica  $C_j$  of at least one of the x blocks  $B_i$ ,  
as a block replica to be used when executing said program.

30 According to a second object of the present invention,  
this solution is characterized in that the securing method  
comprises the steps of:

- creating, within said memory area, M replicas  $C_j$   
( $j = 1, \dots, M$ ) of x program code blocks  $B_i$  ( $x = 1, \dots,$   
35  $N$ ), wherein said replicas reside at different addresses  
within said memory area, and

- randomly selecting one replica  $C_j$  of at least one of the  $x$  blocks  $B_i$ , as a block replica to be used when executing said program.

Therefore, as explained in detail below, the device according to the invention prevents forgery by making the analysis of the electrical signatures very difficult to analyze by such forgery, taking advantage of the fact that said electrical signature varies, in particular, as a function of the values transiting over said device bus lines.

Other features and advantages of the invention will become apparent from the following description of preferred embodiments of the present invention, provided by way of non-limiting examples, in reference to the appended Figures, in which:

Fig. 1 illustrates an integrated circuit device, such as, for example, an electronic component-carrying card.

Fig. 2 illustrates a memory area in the card of Fig. 1.

Fig. 3 illustrates bus lines in the card of Fig. 1.

Fig. 4 illustrates the memory area of Fig. 2 restricted to code block  $B_i$ .

Fig. 5 illustrates addressing of a code block and its replicas within the card of Fig. 1.

Fig. 6 illustrates a distribution of a code block and its replicas within a memory area of Fig. 2.

Fig. 7 illustrates another distribution of a code block and its replicas within the memory area of Fig. 2.

Fig. 1 shows an integrated circuit device 10, for example an electronic component-carrying card.

Card 10 includes a controller (for example a central processing unit or CPU), a memory area 12 including a data memory 14 and a program memory 15, and a terminal block 13 for electrical connection, for example, to a card reader connector.

Memory area 12 is shown in Fig. 2. It contains a program  $P$  including  $N$  code blocks  $B_i$  ( $i = 1, \dots, N$ ) forming code blocks representing steps or operations to be performed when executing said program  $P$ , which enables

performing operations such as reading or selecting data from card 10 and wherein said blocks  $B_i$  handle data and address information.

When executing program P, information interchanges take place between memories 14, 15 and controller 11, through bus lines within said integrated circuit, which are handled by controller 11 in said card 10. The bus lines are either lines for transferring address information, or lines for transferring data information. As shown in Fig. 3, data bus lines D1, D2, ..., D8 and address bus lines A1, A2, ..., A16 are connected to each of the data memory 14 and program memory 15 within each memory area 12 as well as to controller 11 (CPU).

In order to scramble the analysis of the electrical signature on execution of program P, which execution is a sign of card 10 being active, according to the present invention, the device comprises M replicas  $C_j$  ( $j = 1, \dots, M$ ) of one or several blocs  $B_i$  within said memory area 12, and selection means  $M_s$  for randomly selecting one of replicas  $C_j$  of a block  $B_i$  as a block replica to be executed when the latter must be executed within said program P. When program P is executed, several code blocks  $B_i$  will be executed. Fig. 4 illustrates an example for a given block  $B_i$ . For each execution of this block  $B_i$  to be executed within program P and including replicas  $C_j$  within memory area 12, selection means  $M_s$  randomly selects either block  $B_i$  or one of its replicas  $C_j$  so as to execute it within program P. As the various replicas  $C_j$  as well as block  $B_i$  reside at different address values, on each new request for executing block  $B_i$  within program P, the bus lines do not carry the same address values and this makes analyzing the electrical signature, which varies according to the values transiting over the bus lines in card 10, much more difficult. The more replicated blocks  $B_i$  this device includes, the more difficult the signature will be to analyze. This is the reason why the invention provides replicas  $C_j$  for x blocks  $B_i$  ( $x = 1, \dots, N$ ).

In particular, the electrical signature varies as a function of the values transiting over the address bus lines shown in Fig. 3, and more specifically, whenever information 1 is present on a bus line, which information requires a certain electrical current. However, if address values of the above-mentioned replicas  $C_j$  and said replicated block  $B_i$  are equivalent in terms of electrical consumption (for example their values 1111100000000000 and 0000111011000000 induce the same consumption since they each have the same number of bits equal to one and zero), the electrical signature will not change much. Thus, addresses are selected in such a way that the sum of bit values of at least two addresses among the set of addresses of a replicated block  $B_i$  and its  $M$  replicas  $C_j$  are different. In practice, it has been found that, generally speaking, a 1-bit difference among these sums was sufficient for differentiating the various electrical consumption amounts of the address values and therefore make the analysis of the electrical signature more complex. The example illustrated in Fig. 5 shows a block  $B_i$  with its three replicas  $C_1$ ,  $C_2$  and  $C_3$  and their respective addresses  $A_b$ ,  $A_{c1}$ ,  $A_{c2}$  and  $A_{c3}$ . In this example, it can be seen that the bit sums of address values  $A_b$ ,  $A_{c1}$ , and  $A_{c3}$  are different and therefore, that the address values vary in electrical consumption whereas the bit sums of address values  $A_b$  and  $A_{c2}$  are equivalent (with their sum equal to seven) and that, as a consequence, their address values are equivalent in terms of electrical consumption.

Just as the electrical signature varies according to the values transiting over the address bus lines, the electrical signature varies according to the values transiting over the data bus lines shown in Fig. 3.

Thus, according to the present invention, among the set of addresses within a replicated block  $B_i$  and its  $M$  replicas (where block  $B_i$  includes operations for managing a given number of data), an address resides within program memory 15 and another address resides within data memory 14, as shown in the examples of Figs. 6 and 7. In this



respect, the execution of an operation, for example a read or write operation, residing in program memory 15, does not consume the same amount of current as when said operation resides in data memory 14. Operations of the replicated block Bi are seen from card controller 11 as data information transiting over the data bus lines.

Therefore, the above-mentioned system, where blocks are replicated within different memories, enables scrambling of the electrical signature, and it will be understood that this system, in combination with what has been described so far, makes the electrical signature even more difficult to analyze.

Finally, in addition to a random variation of the electrical signature due to the different systems provided within the device according to the present invention and as disclosed previously, the latter provides a random time variation of said signature. More specifically, the present invention provides a device comprising controller means for randomly scheduling the execution of blocks Bi. Each block comprises a set of operations relating to the electronic component-carrying card. These operations, when executed, invoke functions that are managed by card controller 11. For performing these functions, the controller takes time. In general, for each set of functions, the time consumed will be different, which is also the case for each set of operations. Thus, when using this controller means for random execution of blocks, on each new execution of program P, the electrical signature will vary in time since the code blocks are not executed in the same order, whereby, for example, a forger will not be able to repeatedly launch the execution of said program P and analyze the electrical signature in order to find matches between various processing operations and each signal or series of signals contained within the electrical signature. It will be noted that no auxiliary device has been added for countering such forgery.

CLAIMS

1. An integrated circuit device containing a memory area that comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks  $B_i$  ( $i = 1, \dots, N$ ), characterized in that said memory area has M replicas  $C_j$  ( $j = 1, \dots, M$ ) of x program code blocks  $B_i$  ( $x = 1, \dots, N$ ), wherein said replicas reside at different addresses within said memory area, and in that said device comprises selection means for randomly selecting one replica  $C_j$  of at least one of the x blocks  $B_i$ , as a block replica to be used when executing said program.

2. A device according to claim 1, characterized in that the sums of bit values of at least two addresses among the set of addresses of one replicated block  $B_i$  and its M replicas  $C_j$  are different.

3. A device according to any preceding claim, characterized in that, among the set of addresses of one replicated block  $B_i$  and its M replicas, one address resides within the program memory and another address resides within the data memory.

4. A device according to any preceding claim, characterized in that it comprises controller means for randomly scheduling block execution.

5. A method for making secure an integrated circuit device containing a memory area, which comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks  $B_i$  ( $i = 1, \dots, N$ ), characterized in that said method comprises the steps of:

- generating, within said memory area, M replicas  $C_j$  ( $j = 1, \dots, M$ ) of  $x$  program code blocks  $B_i$  ( $x = 1, \dots, N$ ), wherein said replicas reside at different addresses within said memory area, and

- randomly selecting one replica  $C_j$  of at least one of the  $x$  blocks  $B_i$ , as a block replica to be used when executing said program.

6. A method according to claim 5, characterized in that said method comprises the additional step of selecting the sums of bit values of at least two addresses among the set of addresses of one replicated block  $B_i$  and its  $M$  replicas  $C_j$  in such a way that they are different.

7. A method according to claims 5 or 6, characterized in that, among the set of addresses of a replicated block  $B_i$  and its  $M$  replicas, an address is selected within the program memory and another address is selected within the data memory.

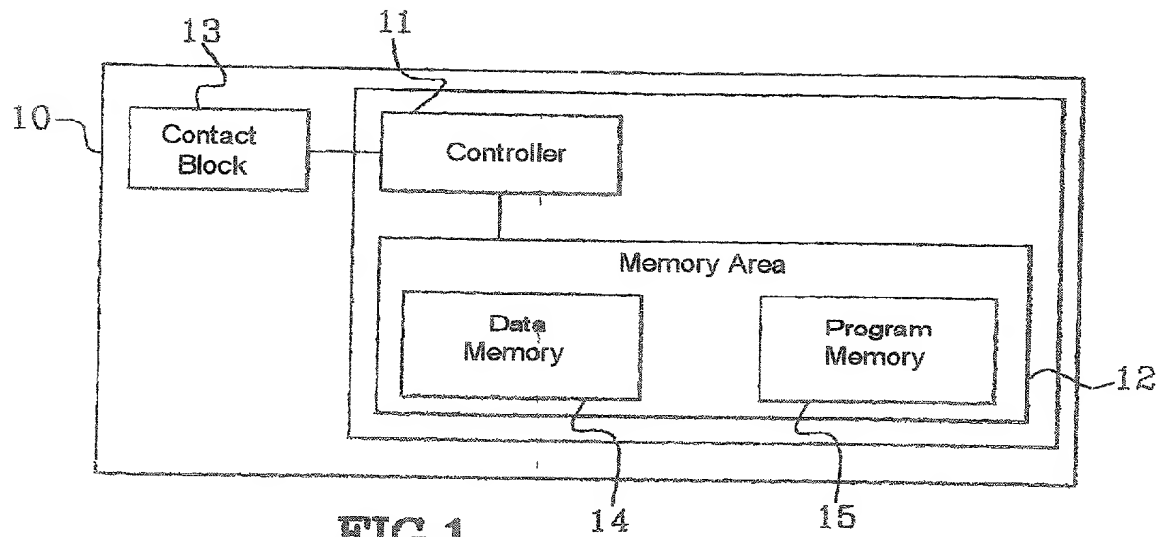
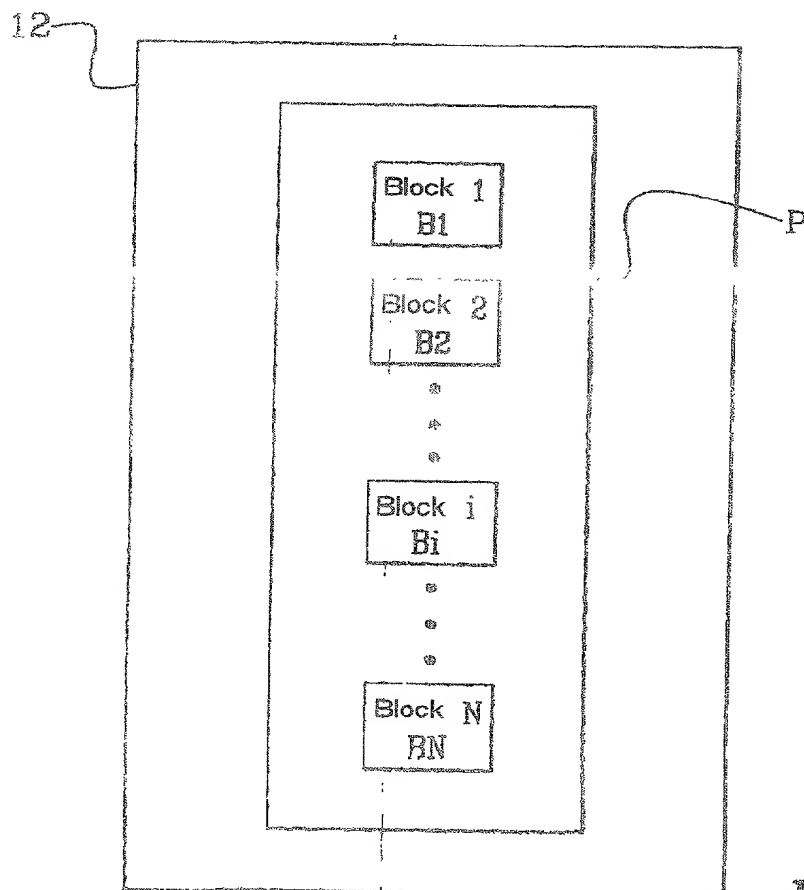
8. A method according to claims 5, 6 or 7, characterized in that said method comprises the additional step of randomly scheduling block execution.

ABSTRACT

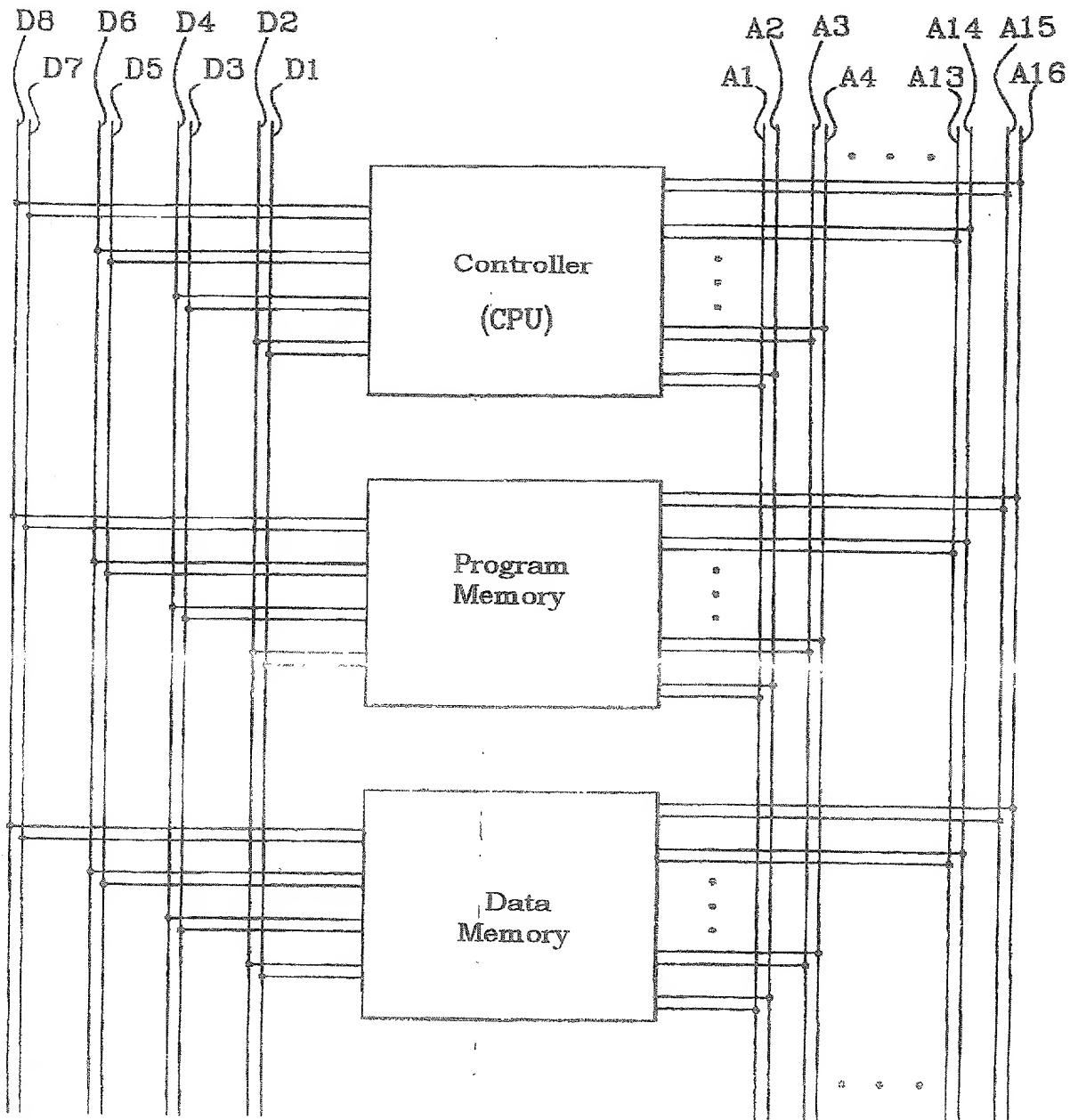
5 The present invention relates to an integrated circuit device containing a memory area, which comprises, on the one hand, a data memory and a program memory, and on the other hand, a program having N code blocks  $B_i$  ( $i = 1, \dots, N$ ). It also relates to a method for making such a device secure. The present invention is characterized in that the memory area has M replicas  $C_j$  ( $j = 1, \dots, M$ ) of x program code blocks  $B_i$  ( $x = 1, \dots, N$ ), which replicas reside at different addresses in said memory area, and in that said device has selection means for randomly selecting one replica  $C_j$  of at least one of the x blocks  $B_i$ , as a block replica to be used when executing said program. In particular, the present invention can be applied to smart cards.

Fig. 4.

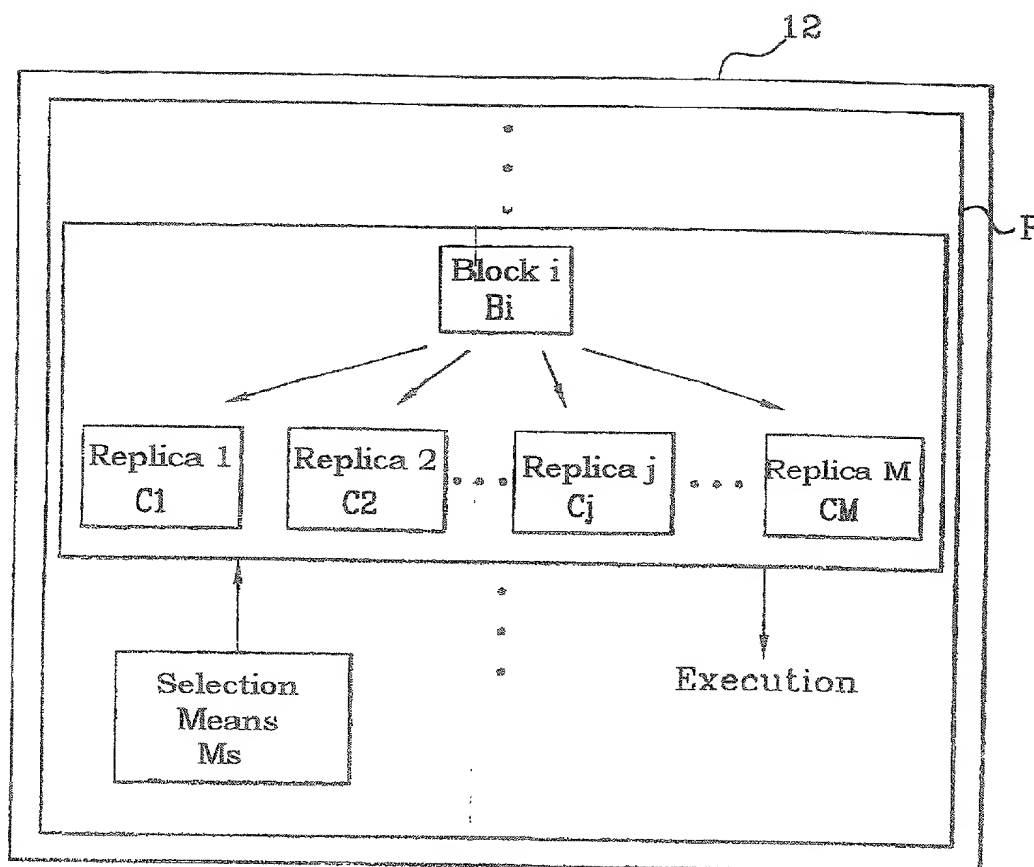
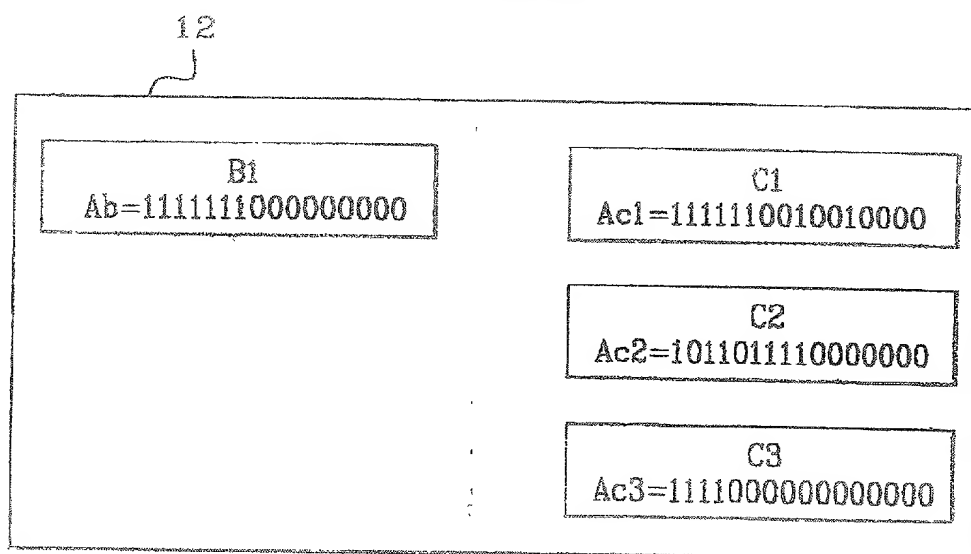
1/4

FIG.1FIG.2

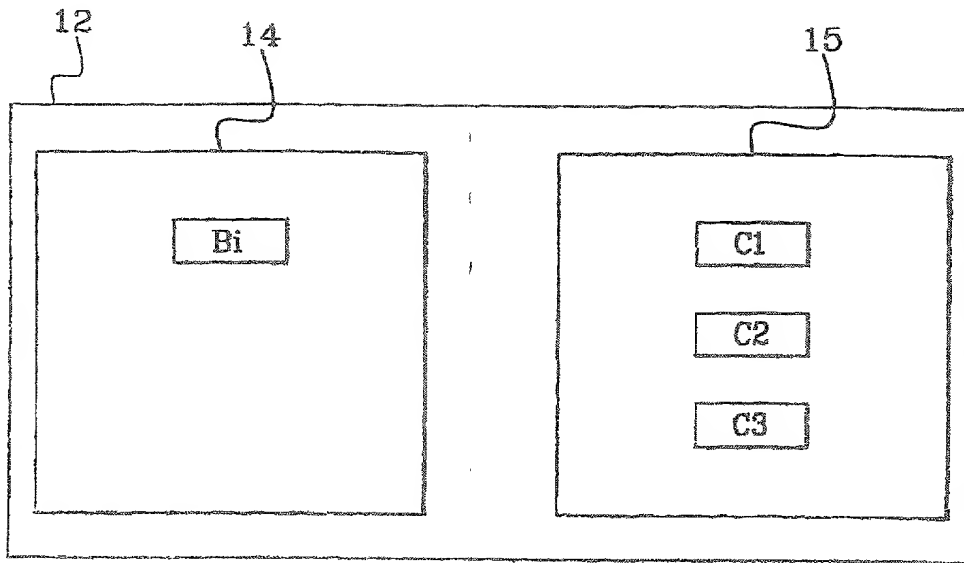
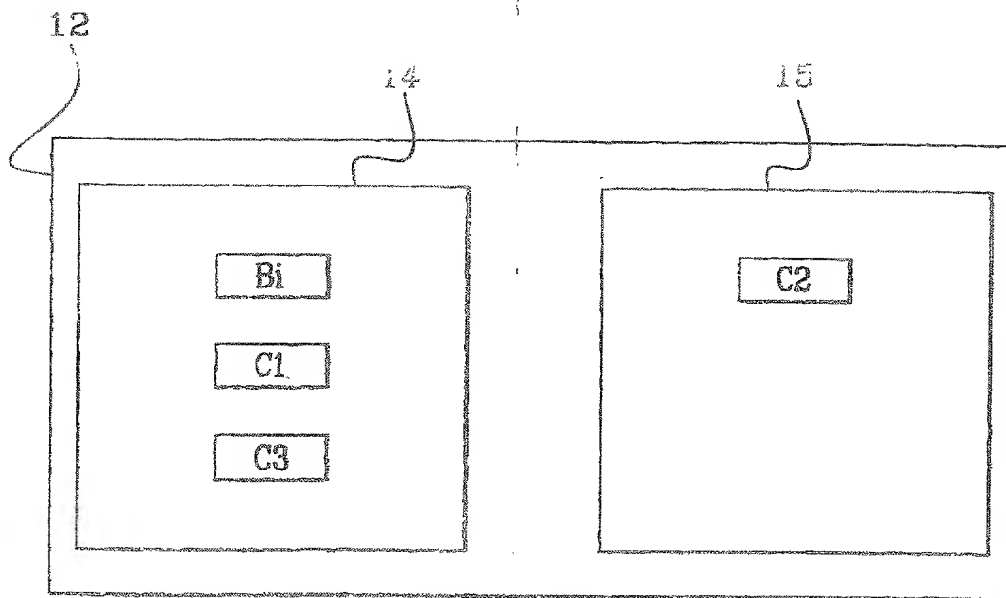
2/4

FIG.3

3/4

FIG. 4FIG. 5

4/4

FIG. 6FIG. 7



Please type a plus sign (+) inside this box → 

PTO/SB/81 (02-01)

Approved for use through 10/31/2002. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

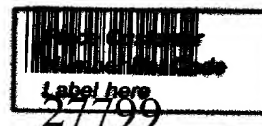
Application Number	09/ 830, 378
Filing Date	April 29, 2001
First Named Inventor	Eric GERBAULT
Title	Device and method for ....
Group Art Unit	
Examiner Name	
Attorney Docket Number	01245/1L

I hereby appoint:

☒ Practitioners at Customer Number

OR

☐ Practitioner(s) named below:



Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number

OR

Place Customer  
Number Bar Code  
Label here

☐ Firm or  
Individual Name

Address

Address

City

State

Zip

Country

Telephone

Fax

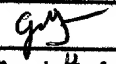
I am the:

☒ Applicant/Inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

### SIGNATURE of Applicant or Assignee of Record

Name	Eric GERBAULT
Signature	
Date	May 15 <sup>th</sup> , 2002

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

☐ \*Total of 1 forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION FOR UTILITY OR  
DESIGN  
PATENT APPLICATION  
(37 CFR 1.63)**

☐ Declaration Submitted with Initial Filing **OR** ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number 01245 / TL

First Named Inventor GERBAULT

**COMPLETE IF KNOWN**

Application Number 09 / 830, 378

Filing Date April 29, 2001

Group Art Unit

Examiner Name

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Device and method for making an integrated circuit secure.

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY)

04/ 29/ 2001

as United States Application Number or PCT International

Application Number 09/ 830, 378 and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
98/ 13606	France	10/ 29/ 1998	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

**Burden Hour Statement:** This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION — Utility or Design Patent Application**Direct all correspondence to: ☒ Customer Number or Bar Code Label ☐ OR ☐ Correspondence address below

Name

Address

City

State

ZIP

Country

Telephone

Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR : ☐ A petition has been filed for this unsigned inventorGiven Name  
(first and middle [if any])

Eric.

Family Name  
or Surname

GERBAULT

Inventor's  
Signature

Date

May 15<sup>th</sup>, 2002

Residence: City

Cachan

State

France  
Country

Citizenship

French

Mailing Address

50, Avenue Jean Jaurès – B.P. 620-12

City

Montrouge Cedex

State

ZIP

92542

Country

France

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this unsigned inventorGiven Name  
(first and middle [if any])Family Name  
or SurnameInventor's  
Signature

Date

Residence: City

State

Country

Citizenship

Mailing Address

City

State

ZIP

Country

☐ Additional inventors are being named on the \_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

09/830378

JC03 Rec'd PCT/PTO 25 APR 2001

Please type a plus sign (+) inside this box → ☐

PTO/SB/122 (10-00)

Approved for use through 10/31/2002. OMB 0651-0035

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**CHANGE OF  
CORRESPONDENCE ADDRESS**  
*Application*Address to:  
Assistant Commissioner for Patents  
Washington, D.C. 20231

Application Number

Filing Date

First Named Inventor

Eric GERBAULT

Group Art Unit

Examiner Name

Attorney Docket Number

01245/TL

Please change the Correspondence Address for the above-identified application to:



Customer Number

01933

Type Customer Number here

OR

Firm or  
Individual Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the :



Applicant/Inventor.

Assignee of record of the entire interest.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

Attorney or Agent of record.

Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number 27,264Typed or Printed  
Name

Thomas Langer, Reg. No. 27,264

Signature

*Thomas Langer*

Date

April 25, 2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.



Total of \_\_\_\_\_ forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

20060501-02000000